Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
United States Department of Justice, Federal	)	RM No. 10865
Bureau of Investigation and Drug	)	
Enforcement Administration	)	
	)	
Joint Petition for Rulemaking to Resolve	)	
Various Outstanding Issues Concerning the	)	
Implementation of the Communications	)	
Assistance for Law Enforcement Act	)	

COMMENTS OF VERISIGN, INC.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Michael Aisenberg
Director of Security Policy
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
Tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Raj Puri
Vice President, NetDiscovery Service
VeriSign Communications Services Div
487 East Middlefield Road
Mountain View CA 94043-4047
tel: +1 510.469.7874
mailto:rpuri@verisign.com

Filed: 12 April 2004

EXECUTIVE SUMMARY

As a leading provider of infrastructure services, VeriSign supports the CALEA regulatory model that relies on industry initiative, combined with the Commission arbitrating and overseeing the implementation of necessary mandates for Law Enforcement. In that spirit, the concerns raised and remedies proposed in the **Joint Petition for Expedited Rulemaking submitted by the United States Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration** (*Joint Petition*) deserve full, comprehensive consideration by the Commission in a rulemaking proceeding. The Joint Petition raises many compelling arguments for acting expeditiously, that include: 1) the rapid network platform changes taking place; 2) the intent of Congress in enacting CALEA; 3) the comprehensive narrow tailoring of the actions sought; 4) the ability of the lawful access support industry to cost-effectively meet these needs today; 5) the minimal adverse effects on new technologies; 6) the consistency of such action with comparable developments occurring worldwide; and 7) the compatibility of such action as a "mandate module" within the Commission's contemplated framework for IP-Enabled Services framework in the *Omnibus Proceeding*.[1]

The immediate declaratory statement sought in the Joint Petition concerning the applicability of CALEA to packet-mode broadband access and telephony services should be considered. Such a statement seems fully consistent with Congress' enactment of CALEA, with previous related Commission findings, and the arguments raised above.

[1] *See IP-Enabled Services*, WC Docket No. 04-36, Notice of Proposed Rulemaking, FCC 04-28 (10 March 2004).

INTRODUCTION

For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted infrastructures that enable signalling, security, identity management, directory, financial transaction, and fraud management capabilities for just about any kind of network based business and consumer services – whether it be Internet, Web, Internet access, traditional voice telephony, VoIP, multimedia, next generation, or sales. VeriSign operates through various divisions that have offices and staff in the U.S. and worldwide. In these various capacities, it participates in scores of different forums, working collaboratively with both industry and government to find entrepreneurial oriented solutions.

As part of these commercial infrastructure support services, VeriSign provides lawfully authorized electronic surveillance (lawful interception) capability requirements to communication providers globally, other lawful access services (i.e., subpoena processing) and participates in or leads many of the related technology, industry, and standards activities.[2] VeriSign also collaborates closely with industry product vendors worldwide directly and through the Global Lawful Interception Industry Association (GLIIF) whose secretariat it hosts.[3] As a result, VeriSign is a significant interested party uniquely positioned to provide perspective and expert comment concerning the *Joint Petition*.

THE CALEA NOTICE OF PROPOSED RULEMAKING

VeriSign's comments for the most part do not address substantive issues raised in the *Joint Petition* – which are properly the subject of the contemplated Notice of Proposed Rulemaking (CALEA NPRM). At issue here are the merits of proceeding expeditiously to that stage, and the comprehensive treatment of the all matters raised in

[2] VeriSign actively participates in the Lawful Interception related standards Technical Committees of the European Telecommunications Standards Institute (ETSI), CableLabs, Organization for the Advancement of Structured Information Standards, Alliance for Telecommunications Industry Solutions, Telecommunications Industry Association, and the Internet Engineering Task Force. It is a founding member of the Global LI Industry forum, a Cisco ecosystem partner for implementing its lawful interception products, a contributor to the expert literature in digital forensics, and an active participant at essentially all law enforcement forums and workshops in this sector.

[3] *See* **Global LI Industry Forum**, http://www.gliif.org

the pleading. The arguments are compelling for this action, and VeriSign urges this occur.

I

RAPIDLY CHANGING NETWORK PLATFORMS COMPEL THIS EXPEDITED RULEMAKING

As the Commission recognized in instituting the IP-Enabled Services proceeding with which this CALEA petition is related,[4] dramatic changes in electronic communication network platforms have occurred over the past several years. Indeed, it is not just the emergence of large-scale IP-enabled Services that are involved here. There are a host of other factors. The technologies and market demand for an always-on world of nomadic users and agile access is supported by a complex network self-configuring terminal devices with globally distributed applications and service providers. Criminals and terrorists who are typically rather nomadic themselves, have gravitated to these technologies on a significant scale.[5]

The digital forensic challenges of pursuing criminal behavior and obtaining evidence have become daunting for even the most expert law enforcement agency. The basic law enforcement support functions sought by Congress in 1994 are being rapidly eroded by these network platform developments. The concerns and remedies raised in the *Joint Petition* are directed at expeditiously making critical adjustments to the capability requirements of network elements pursuant to CALEA provisions, as well as giving due attention to the challenges of implementation and minimizing cost impacts on providers.

II

CONGRESS INTENDED THIS KIND OF RESPONSIVE ACTION

---

[4] *See IP-Enabled Services, supra*.

[5] *See, e.g., e-crime Congress 2004,* National hi-tech Crime Unit, Home Office, UK, http://www.e-crimecongress.org/ecrime2004/website.asp; Institute for Security Technology Studies, Dartmouth College, http://www.ists.dartmouth.edu/ISTS/research_programs.htm; IWS - The Information Warfare Site, http://www.iwar.org.uk/ ; Cybercrime Statistics from the Bureau of Justice Statistics (BJS), http://www.ojp.usdoj.gov/nij/sciencetech/ecrimestats_bjs.htm; *Criminal Exploitation of New Technologies,* Australian Institute of Criminology, http://www.aic.gov.au/publications/tandi/ti93.pdf .

At the time of enacting CALEA, Congress made it plain that the communication network environment was highly dynamic, and that continuing collaborative processes would be necessary among the FCC, the FBI and industry.[6] Indeed, many of the dynamic changes in provisioning and technology platforms are recited repeatedly in the Act's legislative history as the basis for its action and specific mechanisms put in place in 1994.

> The purpose of H.R. 4922 is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies….
>
> To insure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability….
>
> The legislation leaves it to each carrier to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communication can be intercepted at some point that meets the legislated requirements.
>
> Section 2606 establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations.
>
> Carriers can adopt other solutions for complying with the capability requirements….
>
> The FCC retains control over the standards. Under section 2602(b), any carrier, any law enforcement agency or any other interested party can petition the FCC, which has the authority to reject the standards developed by industry and substitute its own.
>
> [T]he absence of standards will not preclude carriers, manufacturers or support service providers from deploying a technology or service, but they must still comply with the assistance capability requirements.
>
> Subsection (b) provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards. Anyone can petition the FCC to establish technical requirements or standards, if none exist, or challenge any such requirements or standards issued by industry associations or bodies under this section.
>
> If an industry technical requirement or standard is set aside or supplanted by the FCC, the FCC is required to consult with the Attorney General and establish a reasonable time and conditions for compliance with and the transition to any new standard. The FCC may also define the assistance obligations of the telecommunications carriers during this transition period.
>
> This section is also intended to add openness and accountability to the process of finding solutions to intercept problems. [7]

[6] *See CALEA Legislative History* at 3495.
[7] *Summary and Purpose, id.*

III

THE ACTION IS NARROWLY TAILORED TO ACHIEVE THE NECESSARY LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE (LAES) CAPABILITIES

The candid concerns and experiences recited in the *Joint Petition* toward implement CALEA capabilities speak to the need for the actions sought in the CALEA NPRM. As mentioned in Sec. I, above, dramatic changes in networks, their deployment and use have occurred. Equally important, lessons have been learned over the past several years since the passage of CALEA about what works and what does not. As noted in Sec. II, above, Congress clearly expected the Commission, as its expert telecommunications agency imbued with broad powers, to evolve the assistance mandates to provide LAES capabilities comparable to those accorded law enforcement since the inception of electronic communications. Today's emerging network environment will deny law enforcement those capabilities unless action is taken.

There are no viable alternatives here. Under extensive and diverse Federal and State statutes, law enforcement has the legal ability to institute LAES. What it lacks is the practical ability to deploy the necessary capabilities at the appropriate Network Elements to accomplish the surveillance within required timeframes.[8] Criminals have the ability to act on a network in microseconds, while law enforcement is encumbered today with solutions that require weeks to institute judicially ordered capabilities. Requiring every law enforcement agency for every approved intercept order to haul equipment around to multiple possible access providers, engineer insertion points, and establish mediation architectures and network connectivity to monitoring facilities, is not a viable course of action. Furthermore, once the voice or other IP-enabled service packets leave the Internet access provider's network, it is essentially impossible to know the routes taken to the destination party of the communication. Interception effectively must occur at the access or application service provider premises.

The only remedy here is Commission CALEA-based action so that the capabilities are in place. The mechanism sought in the Joint Petition seems narrowly

[8] *See, e.g.*, **Cybercrime in New Network Ecosystem: vulnerabilities and new forensic capabilities**, New Crime Scene: The Digital Networked Environment, CyberCrime and Digital Law Enforcement Conference, Yale Law School, 26-28 Mar 2004

crafted in a manner that least affects either new technology or privacy. To the extent anyone believes there are other alternatives to implement such capabilities, the NPRM can serve as a vehicle for suggestions.

IV

THE LAW ENFORCEMENT SUPPORT INDUSTRY VERY COST-EFFECTIVELY PROVIDES THESE CAPABILITIES AS COMMERCIAL SERVICES TODAY

The software, equipment, standards, and support capabilities necessary to meet CALEA packet-mode capabilities are in large measure already available today in the commercial marketplace at reasonable prices. Indeed, the global law enforcement support industry of which VeriSign is part is now focusing on "next generation" developments and emerging challenges, as well as driving down the subpoena processing support costs that generally represent a far greater impact on service providers than CALEA capability costs.[9]

More than two years ago, industry equipment vendors, intercept service providers, and standards bodies began to develop products and services to meet the growing need worldwide to support common law enforcement digital forensic needs for VoIP and IP-enabled services. Because the needs and solutions are inherently international, much of the work was accomplished within the lead international forum - the European Telecommunication Standards Institute (ETSI) Lawful Interception Technical Committee (TC LI), as well as CableLabs and large-scale proprietary initiatives by major vendors.[10]

---

[9] *See, e.g., Lawful Interception of WLAN Internet Access*, ETSI TC LI 05litd068r1 (Mar 2004); *On LI and the market place*, ETSI TC LI 05litd050 (Mar 2004); *Report on OASIS Subscriber Data Handover Interface Specification*, ETSI TC LI 05litd027 (Mar 2004); *Integration and Treatment of VoIP and other IP-Enabled Services LI specifications*, ETSI TC LI 05litd028R3 (Mar 2004); *MetaView Model of IP Interception*, ETSI TC LI-Rap#05TD012 (Jan 2003).

[10] *See, e.g., Technical Specification, Telecommunications security, Lawful Interception (LI), Handover specification for IP delivery*, ETSI TS 102 232 V1.1.1 (2004-02); *Technical Specification, Telecommunications security, Lawful Interception (LI), Service-specific details for internet access services*, ETSI TS 102 234 V1.1.1 (2004-02); *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*, ANSI T1.678-2004 ; *PacketCable Electronic Surveillance Specification*, PKT-SP-ESP-I02-030815 (Nov 2004); *UMTS Handover Interface for Lawful Interception*, ANSI T1.724-2004; *Cisco Architecture for Lawful Intercept In IP Networks*, Doc. draft-baker-slem-architecture-02.txt, Oct 2003; *Cisco Lawful Intercept Control MIB*, Doc. draft-baker-slem-mib-00, Apr 2003; *Technical Specification, Universal Mobile Telecommunications System (UMTS), 3G security, Handover interface for Lawful Interception (LI)*, (3GPP TS 33.108 version 5.6.0 Release 5),

Law enforcement forums and participation from many different countries occurred.[11] Standards and products were produced, tested, and implemented.

VeriSign is particularly pleased in having participated in many of these forums with dozens of contributions, facilitated collaboration within the industry, tested vendor solutions, and implemented CALEA outsource support offerings to customers in the form of NetDiscovery Service™ to major broadband access providers. See Attachment A - *VeriSign NetDiscovery Services Implemented by Cox Communications to Meet CALEA Compliance Requirements.*

Although VeriSign regards itself as the industry services leader - a competitive marketplace exists with other providers to choose from, both domestically and internationally. Additionally, the really significant levels of efficiency, technology evolution, implementation speed, high availability, increased security, cost reduction, accountability and privacy enhancement possible through service bureau intermediaries between the large number of communication service providers and law enforcement agencies today, make such services a highly compelling and sustaining value proposition for all parties in the process.

However, notwithstanding the need and availability of solutions, what is missing at the moment is the attention to coverage, compliance, and costs raised in the *Joint Petition* to achieve the deployment necessary to meet the needs of law enforcement within the scope of CALEA.

V

NEW TECHNOLOGIES WILL NOT BE ADVERSELY AFFECTED

None of the techniques deployed or standardized over the past several years to accomplish lawful interception of Internet access, IP-Enabled or VoIP services adversely affect the evolution or deployment of those services. These techniques include: 1) isolated adjunct devices that passively duplicate transmission streams and actively filter target communications, 2) Simple Network Management Protocol (SNMP) or

---

ETSI TS 133 108 V5.6.0 (2003-12); *Lawful Intercept for cdma2000 Voice over Packet (VoP),* TR45.6 Doc. 20030915003 Nortel-LI-VoP.pdf

[11] ETSI LI participants include representatives from Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Israel, Italy, The Netherlands, Norway, Russia, Spain, Sweden, Switzerland, UK, USA

Operating System based means of creating duplicating copies the target communications in network devices, or 3) agent or active probe devices at network elements replicate target communications. Most of these techniques were developed for network or traffic management purposes and have a dual use of meeting lawful interception capability requirements, and a competitive marketplace among alternative technology vendors exists. Where the techniques are "outboard" – they have no effect on performance of any other network device. Where the techniques are embedded in a network device, they have minimal performance effects at the low levels of intercepts typically originated by law enforcement orders.

Furthermore, since LI capability requirements for Internet infrastructure equipment are essentially a global fact of life today for vendors, the necessary techniques have been implemented or provided for by most major product vendors. The implementations include a mixture of proprietary or open standards that mediation equipment and LI service bureau vendors have attempted to support to meet the needs of law enforcement monitoring centers.

Fears or arguments that the imposition of CALEA requirements on Internet access or IP-enabled services will retard or impede deployment or innovation are neither plausible nor borne out by the facts.

VI

THE CONTEMPLATED ACTIONS ARE COMPARABLE AND COMPATIBLE WITH DEVELOPMENTS OCCURRING WORLDWIDE BY REGULATORY AUTHORITIES, INDUSTRY AND LAW ENFORCEMENT

Although the Joint Petition is predominantly focused on the needs of the petitioners' and other U.S. law enforcement agencies, the needs being served – especially for packet-oriented and IP-enabled Services – are basically global in nature.[12] The services and network architectures are distributed worldwide. The criminal and terrorist activities being investigated and digital forensic evidence being collected are occurring in almost every country. As noted above, the solutions are being addressed in an array of

[12] *See, e.g.*, n. 5, *supra; Technical Specification, Telecommunications security, Lawful Interception (LI), Requirements of Law Enforcement Agencies*, ETSI TS 101 331 V1.1.1 (2001-08)

global collaborative law enforcement, regulatory and industry forums. Indeed, some of the greatest emerging challenges today deal with CALEA and similar provisions in other countries as applied to transnational service providers.[13]

Also relevant is the Convention on Cybercrime which comes into force on 1 July 2004. The U.S. played a leading role in bringing about this treaty instrument.[14] It is also a signatory and in the process of ratification.[15]

While many of the provisions of the Convention may deal with information services as that term is used within CALEA, some of those provisions deal with convergent communications that could properly fall within the ambit of the Act. In this respect, CALEA provisions will serve to further the fulfillment of U.S. obligations assumed under the Convention on Cybercrime.

In and among other countries, however, the Convention is a significant driver of increasing international cooperation in bringing about common standards and capabilities for the production of real-time communications data along the lines sought in the Joint Petition.

The actions being sought in the Joint Petition are not only fully consonant with similar actions occurring in other countries and international forums, but also crafted so as to leverage recently adopted and implemented international Lawful Interception standards that will drive down related equipment costs.

---

[13] *See, e.g., Jurisdictional and Other Concerns Associated with Satellite System Communications Services When System Earth Station Gateways Are Located in a Foreign Country: toward effective global lawful access and interception arrangements*, ETSI, Doc. iuradhoc014 (20 Jan 2004)

[14] *See, e.g.*, Stephen J. Lukasik, Lawrence T. Greenberg, Seymour E. Goodman, **Protecting an invaluable and ever-widening infrastructure**, 41 Communications of the ACM 6 (June 1998); Abraham D. Sofaer, Seymour E. Goodman, Stephen J. Lukasik, et al, **A Proposal for an International Convention on Cyber Crime and Terrorism**, The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP), The Center for International Security and Cooperation (CISAC), Stanford University, http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm, August 2000; Lukasik et al, in **The Transnational Dimension of Cyber Crime and Terrorism**, Abraham D. Sofaer and Seymour E. Goodman, editors, Hoover Institution, 2001; Stephen Lukasik , Seymour Goodman , David Longhurst, **National Strategies for the Protection of Critical Infrastructures Against Cyber Attack**, Oxford University Press (October, 2003).

[15] Message from the President of the United States, Senate Treaty Doc. 108-11, 108th Congress 1st Session, 17 Nov 2003.

VII

THE RULEMAKING PETITION IS CONSISTENT AS A "MANDATE MODULE" WITHIN THE COMMISSION'S CONTEMPLATED FRAME-WORK FOR IP-ENABLED SERVICES

The Commission's "omnibus" IP-Enabled Services regulatory proceeding casts a comprehensive, fundamentally important new framework, seeking…

> …comment on the impact that IP-enabled services, many of which are accessed over the Internet, have had and will continue to have on the United States' communications landscape. As a truly global network providing instantaneous connectivity to individuals and services, the Internet has transcended historical jurisdictional boundaries….[16]

In articulating this new framework, the Commission in the NPRM as well as statements of individual commissioners, expressly defer to the instant petition as an integral dimension of the public safety obligations treated in that proceeding, recognizing…

> The Commission recognizes the importance of ensuring that law enforcement's requirements are fully addressed. The Commission takes seriously the issues raised by law enforcement agencies concerning lawfully authorized wiretaps. Accordingly, the Commission plans to initiate a rulemaking proceeding in the near future to address the matters we anticipate will be raised by law enforcement, including the scope of services that are covered, who bears responsibility for compliance, the wiretap capabilities required by law enforcement, and acceptable compliance standards.[17]

The proposed Joint Petition actions closely match not only the exercise of regulatory authority contemplated in the IP-Enabled Services NPRM, but also the treatment of CALEA support services as a billed public safety obligation similar to 911 services. Such line item billing has the additional benefit of providing transparency as to the costs of CALEA compliancy – also an objective long sought by the Commission and Congress.

[16] *IP-Enabled Services, supra,* at para. 1
[17] *Id* at para. 50, n. 158.

DECLARATION THAT PACKET-MODE BROADBAND ACCESS AND TELEPHONY SERVICES ARE SUBJECT TO CALEA

The Joint Petition asks the Commission "to reaffirm that packet-mode communications services are subject to CALEA," and "to initially issue a Declaratory Ruling or other formal Commission statement, finding that…CALEA applies to two closely related packet-mode services…broadband access service and broadband telephony service."[18] The term broadband access is meant "to refer to the process and service used to gain access or connect to the public Internet using a connection based on packet mode technology that offers high bandwidth."[19] Broadband telephony refers "to the transmission or switching of voice communications using broadband facilities."[20]

The Joint Petition suggests a combination of broadband access coupled with "mediation" as the basis for declaring CALEA responsibility for broadband telephony. This nexus to mediation is used to distinguish mediated offerings from pure peer-to-peer voice communication. Multiple arguments are provided that underscore the equivalency to public switched telephone service (PSTN) and the compelling need for immediate declaratory action.

Broadband Access.

With respect to broadband access, the request for a declaration almost paraphrases the CALEA legislative history text and the intent is clear:

> a carrier providing a customer with a service or facility that allows the customer to obtain access to a publicly switched network is responsible for complying with the capability requirements. [and] recognizes, however, that law enforcement will most likely intercept communications over the Internet at the same place it intercepts other electronic communications: at the carrier that provides access to the public switched network.[21]

The technology, standards, and equipment exist to accomplish this capability requirement at reasonable cost. Such capabilities are offered as a VeriSign NetDiscovery Service. VeriSign therefore supports such a declaration.

---

[18] *Joint Petition* at 8, 15.
[19] *Idem*.
[20] *Idem*.
[21] *CALEA Legislative History, supra.*

There are, however, an exceedingly wide variety of providers of these services – ranging from a small café owner to Tier 1 local exchange and wireless carriers or cable systems. However, it is often these kinds of access facilities most favored by criminals and terrorists. VeriSign believes that simple, cost-effective CALEA support solutions also exist for small-scale local providers and is pursuing them in the commercial marketplace.

Broadband Telephony

With respect to broadband telephony, the request for a declaration also closely paraphrases CALEA legislative history text and the intent is clear:

> the capability requirements only apply to those services or facilities that enable the subscriber to make, receive or direct calls.[22]

The technology, standards, and equipment exist to accomplish this capability requirement at reasonable cost. VeriSign already provides CALEA services for precisely this kind of broadband telephony, and supports a declaration.

[22] *Idem*

VeriSign NetDiscovery Services Implemented by Cox Communications

Service Tested and Implemented in advance of new FCC Rules to Broaden CALEA Ruling to Include VoIP and Broadband Internet Services

Mountain View, CA. – April 5, 2004 - VeriSign, Inc. (Nasdaq: VRSN), the leading provider of critical infrastructure services for the Internet and telecommunications networks, and Cox Communications, a multi-service broadband communications company with approximately 6.6 million total customers, today announced that Cox has implemented VeriSign NetDiscovery™ Services to help ensure compliance of its Voice over Internet Protocol (VoIP)-based cable telephony services with the Communications Assistance for Law Enforcement Act (CALEA). Cox Communications launched its 12th telephony market in December 2003 in Roanoke, Va., and its first using VoIP technology. Eleven other Cox systems offer Cox Digital Telephone using circuit-switched technology, all CALEA-compliant since first introduced in 1997.

VeriSign NetDiscovery Services, which was tested and implemented to support the Cox data network infrastructure used in VoIP deployments, assists Cox in meeting CALEA compliance through an outsourced model of service, which will minimize Cox's capital and operational expenditures. To implement the service, VeriSign worked with the VoIP network infrastructure vendors supplying to Cox and integrated the end-to-end NetDiscovery solution.

Cox's announcement underscores VeriSign's commitment and ability to provide carriers and service providers with the necessary services they need to introduce integrated next-generation communications services and comply with CALEA. This announcement also marks VeriSign's first CALEA compliance implementation with a major cable provider. VeriSign will utilize its heritage in security, Internet infrastructure and telecommunications to aid cable providers via a unique managed communications services model to quickly deliver the integrated, next-generation services that wireless, cable and wireline subscribers are demanding.

"VeriSign provides a full spectrum of other tools and services aimed at top-tier carriers, including NetDiscovery," said Bill Dame, director of network switch engineering at Cox Communications. "Cox has always considered CALEA compliance as a top priority in our circuit switched markets, and realized that CALEA in new markets served by VoIP would be a challenge. VeriSign came in with a total solution, using the same equipment we had evaluated, and made it easy and cost effective."

Vernon Irvin, executive vice president of VeriSign Communications Services, said: "Being the leader in managed security services, VeriSign is delivering a service via its NetDiscovery

platform to Cox Communications in order to assist them with CALEA compliance. VeriSign can help all types of service providers meet their legal obligations both securely and at a low cost."

CALEA requires carriers to assist Law Enforcement Agencies (LEAs) in lawfully authorized surveillance. To comply, carriers often have to purchase dedicated hardware, have trained operation staff and are called upon to maintain connectivity with a variety of LEAs. VeriSign's NetDiscovery Service greatly streamlines the CALEA compliance requirements and eliminates the need to purchase costly equipment.

The service offers a secure and streamlined administration, along with a multitude of connectivity options that make it easy to fulfill lawful interception mandates and take the burden and expense of compliance out of a service provider's hands. By outsourcing the service to VeriSign, service providers maintain continuous, hassle-free compliance.

Greg Caressi, vice president of Frost & Sullivan said: "It used to be that to satisfy regulations, a carrier had to do it themselves. VeriSign's NetDiscovery Service offers carriers a safe, secure and trusted way to reach CALEA compliance without having to utilize a great deal of internal resources."

For more information on VeriSign's NetDiscovery
http://www.verisign.com/telecom/products/network/netDiscovery.html

About VeriSign
VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. Additional news and information about the company is available at http://www.verisign.com.

For more information, contact:
VeriSign Media Relations: Leslie Rubin, lrubin@verisign, 650-426-5363
VeriSign Investor Relations: Kathleen Bare, kbare@verisign.com, 650-426-3241

###